ABSTRACT

In a method for verifying, by a verifier, that a prover has access to a private key associated with a public key Kp, in which the method comprises the prover generating a random number R and communicating a disguised form of the random number R to the verifier, an improvement including the prover generating the random number R based on an input received from the verifier.

Related apparatus and methods are also provided.